

MS221 CB D



The Open
University

A second level
interdisciplinary
course

Exploring **Mathematics**

COMPUTER BOOK

D

BLOCK D

STRUCTURE IN MATHEMATICS

Computer Book D

M5221 CB D



The Open
University

A second level
interdisciplinary
course

Exploring **Mathematics**

COMPUTER BOOK

D

BLOCK D

STRUCTURE IN MATHEMATICS

Computer Book D

Prepared by the course team

About this course

This computer book forms part of the course MS221 *Exploring Mathematics*. This course and the courses MU120 *Open Mathematics* and MST121 *Using Mathematics* provide a flexible means of entry to university-level mathematics. Further details may be obtained from the address below.

MS221 uses the software package Mathcad (MathSoft, Inc.) to investigate mathematical concepts and as a tool in problem solving. This software is provided as part of the course.

This publication forms part of an Open University course. Details of this and other Open University courses can be obtained from the Course Information and Advice Centre, PO Box 724, The Open University, Milton Keynes, MK7 6ZS, United Kingdom: tel. +44 (0)1908 653231, e-mail general-enquiries@open.ac.uk

Alternatively, you may visit the Open University website at <http://www.open.ac.uk> where you can learn more about the wide range of courses and packs offered at all levels by The Open University.

To purchase a selection of Open University course materials, visit the webshop at www.ouw.co.uk, or contact Open University Worldwide, Michael Young Building, Walton Hall, Milton Keynes, MK7 6AA, United Kingdom, for a brochure: tel. +44 (0)1908 858785, fax +44 (0)1908 858787, e-mail ouwenq@open.ac.uk

The Open University, Walton Hall, Milton Keynes, MK7 6AA.

First published 1997. Second edition 2004.

Copyright © 2004 The Open University

All rights reserved; no part of this publication may be reproduced, stored in a retrieval system, transmitted or utilised in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without written permission from the publisher or a licence from the Copyright Licensing Agency Ltd. Details of such licences (for reprographic reproduction) may be obtained from the Copyright Licensing Agency Ltd, 90 Tottenham Court Road, London W1T 4LP.

Open University course materials may also be made available in electronic formats for use by students of the University. All rights, including copyright and related rights and database rights, in electronic course materials and their contents are owned by or licensed to The Open University, or otherwise used by The Open University as permitted by applicable law.

In using electronic course materials and their contents you agree that your use will be solely for the purposes of following an Open University course of study or otherwise as licensed by The Open University or its assigns.

Except as permitted above you undertake not to copy, store in any medium (including electronic storage or use in a website), distribute, transmit or re-transmit, broadcast, modify or show in public such electronic materials in whole or in part without the prior written consent of The Open University or in accordance with the Copyright, Designs and Patents Act 1988.

Edited, designed and typeset by The Open University, using the Open University TeX System.

Printed and bound in the United Kingdom by The Charlesworth Group, Huddersfield.

ISBN 0 7492 6650 3

Contents

| | |
|---------------------------------------|----|
| Guidance notes | 4 |
| Chapter D1 | 5 |
| Section 6 Complex numbers and Mathcad | 5 |
| 6.1 Complex arithmetic in Mathcad | 5 |
| 6.2 Finding roots with Mathcad | 8 |
| 6.3 Complex exponentials and geometry | 12 |
| Chapter D2 | 17 |
| Section 5 Number theory and Mathcad | 17 |
| 5.1 The Division Algorithm | 17 |
| 5.2 Remainders of powers | 19 |
| 5.3 Arithmetic in \mathbb{Z}_n | 22 |
| 5.4 Multiple precision arithmetic | 25 |
| Chapter D3 | 27 |
| Section 1 Symmetry | 27 |
| 1.3 Using symmetries | 27 |

Guidance notes

This computer book contains those sections of the chapters in Block D which require you to use Mathcad. Each of these chapters contains instructions as to when you should first refer to particular material in this computer book, so you are advised not to work on the activities here until you have reached the appropriate points in the chapters.

In order to use this computer book, you will need the following Mathcad files.

Chapter D1

- 221D1-01 Cartesian and polar forms
- 221D1-02 Roots of unity
- 221D1-03 Complex exponentials (Optional)

Chapter D2

- 221D2-01 Remainders of powers
- 221D2-02 Modular arithmetic

Chapter D3

- 221D3-01 Piecewise linear paths (Optional)
- 221D3-02 PLPs with symmetry (Optional)
- 221D3-03 A rose window (Optional)

Instructions for installing these files onto your computer's hard disk, and for opening them, are given in Chapter A0 of MST121.

Activities based on software vary both in nature and in length. Sometimes the instructions for an activity appear only in the computer book; in other cases, instructions are given in the computer book and on screen. Feedback on an activity is sometimes provided on screen and sometimes given in the computer book.

For advice on how each computer session fits into suggested study patterns, refer to the Study guides in the chapters.

Note that there are no specified computer activities associated with Chapter D4.

Chapter D1, Section 6

Complex numbers and Mathcad

6.1 Complex arithmetic in Mathcad

Certain quadratic equations have roots that are complex numbers, and you may have already seen Mathcad produce such roots in this context. For example, suppose that you use the symbolic keyword 'solve' to solve the equation $x^2 - 6x + 25 = 0$. Mathcad gives the two solutions as

$$\begin{pmatrix} 3 + 4i \\ 3 - 4i \end{pmatrix}.$$

This is as we would expect, since the equation has the two solutions $3 \pm 4i$. Note that Mathcad uses the usual symbol i for $\sqrt{-1}$.

Mathcad will perform various manipulations with complex numbers. To use it for this purpose, you need first to be able to enter complex numbers into Mathcad. (This requires a little care, since Mathcad needs to know when the symbol i is being used to mean $\sqrt{-1}$, rather than in some other way, such as, say, part of a variable name.) For example, to enter $3 + 4i$, you can click on the buttons on the 'Calculator' toolbar, including the i button, or just type $3+4i$. (You do *not* enter a multiplication between the 4 and the i .) However, when i is entered alone in Mathcad, it must be entered as $1i$. This extra '1' in front of the i is entered for you automatically if you click on the i button, but when using the keyboard, you must type $1i$. For example, to enter $2 - i$ via the keyboard, you type $2-1i$. (The '1' is visible only when entering or editing the complex number. It disappears once the number is complete.)

This symbolic keyword was introduced in MST121 Chapter A3; see also *A Guide to Mathcad*.

Activity 6.1 Entering complex numbers in Mathcad

- (a) By hand, simplify each of the following complex numbers.
- (i) $(3 + 4i)(3 - 4i)$ (ii) $i(3 - 4i)$
- (b) Create a new (Normal) worksheet. Then enter each of the complex products in part (a), and enter $=$ to evaluate them.

Comment

- (a) These products are
- (i) 25; (ii) $4 + 3i$.
- (b) Mathcad gives the above values. If you use keyboard entry, and type i or $1*i$ to enter i in (ii), then Mathcad gives an error, treating i as an undefined variable, not as $\sqrt{-1}$. The key sequence required here is $1i*(3-4i)$. (Whatever entry method you use for (ii), you *must* enter the multiplication between the i and the left bracket – Mathcad will *not* insert it if you omit to do so.)

The next activity provides further practice in entering complex numbers.

Activity 6.2 Multiplying complex numbers

- (a) By hand, evaluate $(1 - 2i)(3 + 4i)$.
- (b) On a new (Normal) worksheet, enter the expressions shown below. For each of zw and $(ac - bd) + (ad + bc)i$, click on the expression and then enter $=$ to evaluate it. Experiment with other values of a , b , c and d , if you wish.

$$\begin{array}{llll} a := 1 & b := -2 & c := 3 & d := 4 \\ z := a + bi & w := c + di & & \\ zw & & & \\ (ac - bd) + (ad + bc)i & & & \end{array}$$

Comment

- (a) This product is $11 - 2i$, as Mathcad confirms.
- (b) The two expressions give the same value whatever values are specified for a , b , c and d , as one would expect!

Leave this worksheet open; it will be used again for the next activity.

Mathcad can evaluate the real and imaginary parts of a complex number, complex conjugates and the modulus of a complex number. It uses the usual notations: $\text{Re}(z)$ for the real part of z , $\text{Im}(z)$ for the imaginary part of z , \bar{z} for the complex conjugate of z , and $|z|$ for the modulus of z . To enter the first two, one just types the expressions $\text{Re}(z)$ or $\text{Im}(z)$. To enter \bar{z} , type $z[\text{Shift}]2$. To enter $|z|$, type z , then click on the $|x|$ button on the 'Calculator' toolbar or use the keyboard alternative $[\text{Shift}]\backslash$.

Activity 6.3 Complex arithmetic

- (a) With the complex numbers $z = 1 - 2i$ and $w = 3 + 4i$ entered on a worksheet, as you did for the previous activity, use Mathcad to calculate each of (i)–(ix) below.
- (i) $z + w$ (ii) $w + z$ (iii) $\text{Re}(z)$ (iv) $\text{Im}(w)$ (v) \bar{z}
 (vi) $|w|$ (vii) $1/w$ (viii) w/z (ix) $w\bar{z}/|z|^2$
- (b) Try varying a , b , c and d , and check that (viii) and (ix) in part (a) give the same answers each time.

Comment

- (a) Mathcad gives the following answers.

$$\begin{array}{llllll} \text{(i)} \ 4 + 2i & \text{(ii)} \ 4 + 2i & \text{(iii)} \ 1 & \text{(iv)} \ 4 & \text{(v)} \ 1 + 2i & \text{(vi)} \ 5 \\ \text{(vii)} \ 0.12 - 0.16i & \text{(viii)} \ -1 + 2i & \text{(ix)} \ -1 + 2i & & & \end{array}$$

- (b) We have $z \times \bar{z} = |z|^2$ (see Exercise 3.2(b)), and so

$$w/z = w\bar{z}/z\bar{z} = w\bar{z}/|z|^2.$$

Mathcad should therefore give the same values for w/z and for $w\bar{z}/|z|^2$, for any complex numbers w and z (where $z \neq 0$).

Remember, to enter $a + bi$, use the buttons on the 'Calculator' toolbar or type $a+b*i$. (Note that, when variables are used to construct a complex number, a multiplication $*$ is required before the i , which must be typed as $1i$.)

Remember that names are case sensitive in Mathcad. You *must* use capital R and I here.

Mathcad notes

- ◇ $\text{Re}(z)$ and $\text{Im}(z)$ are built-in Mathcad functions. As well as typing them directly, you can also enter them by selecting **Function...** from the **Insert** menu. Choose 'Complex Numbers' from the 'Function Category' box, then either 'Re' or 'Im' from the 'Function Name' box, before clicking on 'Insert'.
- ◇ The double-quote " (obtained by typing [Shift]2) performs several roles in Mathcad. When entered *after* an expression (selected within the blue editing lines) it applies the complex conjugate operator to that expression. However, when " is entered in an empty space in the worksheet (at the red cross cursor) it creates a text region, and when entered in an empty placeholder in an expression it creates a text string variable.

Remember that Mathcad notes are *optional*.

We look next at Argand diagrams, and at translating between the polar and Cartesian forms of a complex number. Mathcad file 221D1-01 provides templates for translating between the two forms. It also shows Mathcad plots illustrating each of these forms.

Activity 6.4 Polar and Cartesian forms

Open Mathcad file **221D1-01 Cartesian and polar forms**, and turn to page 2 of the worksheet. Here a and b are the real and imaginary parts of the complex number z , whose Cartesian form is $z = a + bi$. The corresponding polar form is $\langle r, \theta \rangle$, where $r = |z|$ and θ is defined by the Mathcad expression $\arg(z)$, of which more below. In the polar form, θ is by default in radians, but θ is also shown in the worksheet in degrees (which is usually easier to visualise). The page also shows Argand diagram plots illustrating each of the Cartesian and polar forms.

You will not be asked to create such Mathcad plots. (For your interest only, details of how to do so are provided on page 4 of the worksheet.)

- (a) Working by hand, express each of the complex numbers (i)–(iv) below in polar form.
(i) $2 - 2i$ (ii) -5 (iii) $3i$ (iv) $-2 - 2i$
- (b) Check that Mathcad gives in each case the result for the polar form that you calculated in part (a). In what range do the values that Mathcad gives for $\arg(z)$ lie?
- (c) Use the worksheet to obtain the polar form of $3 - 8i$.
- (d) Given a complex number $\langle r, \theta \rangle$ in polar form, whose Cartesian form is $a + bi$, what are its real part a and imaginary part b ?
- (e) Turn to page 3 of the worksheet, which gives a template for converting from polar to Cartesian form. Check that the equations used here are as you would expect. Use this template to express each of the following in Cartesian form.
(i) $\langle 3, \pi \rangle$ (ii) $\langle 2, 2.1 \rangle$

Comment

- (a) We obtain the following polar forms.
(i) $\langle 2\sqrt{2}, -\frac{1}{4}\pi \rangle$ (ii) $\langle 5, \pi \rangle$ (iii) $\langle 3, \frac{1}{2}\pi \rangle$ (iv) $\langle 2\sqrt{2}, -\frac{3}{4}\pi \rangle$

- (b) Above the Argand diagram plots, Mathcad gives the same values that were found in part (a), but expressed as decimals (to 3 decimal places), as follows.

$$(i) \langle 2.828, -0.785 \rangle \quad (ii) \langle 5, 3.142 \rangle \quad (iii) \langle 3, 1.571 \rangle \\ (iv) \langle 2.828, -2.356 \rangle$$

Mathcad also gives exact answers, obtained by using symbolic evaluation (\rightarrow), further down page 2 of the worksheet. Here $\sqrt{2}$ appears as $2^{1/2}$.

The values that Mathcad gives for $\arg(z)$ lie in the range $(-\pi, \pi]$. Thus the Mathcad function \arg gives the principal value of the argument, as defined in Subsection 3.2. (However, when expressed in degrees, these values differ by 360° from those shown on the lower half of the Argand diagram polar plot.)

- (c) You should obtain the polar form $\langle 8.544, -1.212 \rangle$ (to 3 decimal places).
 (d) We have $a = r \cos \theta$ and $b = r \sin \theta$.
 (e) We obtain the following.
 (i) -3 (as we would expect)
 (ii) $-1.010 + 1.726i$ (to 3 decimal places)

Now close file 221D1-01.

6.2 Finding roots with Mathcad

You have met various ways of using Mathcad to solve equations. Solve blocks and the Newton–Raphson method each employ a numerical algorithm, and each will find only one solution at a time. To find all the roots of a polynomial, both real and complex, a different approach is preferable.

Mathcad will give the two roots of a quadratic polynomial, using the symbolic keyword ‘solve’. This works whether the roots are real or complex. The roots are obtained using the formula for the solutions of a quadratic equation, to give exact rather than approximate solutions. If you enter the quadratic with its coefficients given as integers or rationals, then Mathcad gives the roots of the quadratic exactly, using square roots if necessary. If you enter the coefficients as decimals, then Mathcad returns the roots as decimals. Figure 6.1 shows an example. Mathcad initially gives these decimal solutions to 20 places, but if you click on the answer and enter \equiv , it displays the solutions to the number of decimal places specified in ‘Number of decimal places’, on the ‘Number Format’ tab under **Result...** on the **Format** menu.

$$2x^2 + \frac{5}{2}x + \frac{7}{4} \text{ solve, } x \rightarrow \begin{pmatrix} \frac{-5}{8} + \frac{1}{8}i \times 31^{\frac{1}{2}} \\ \frac{-5}{8} - \frac{1}{8}i \times 31^{\frac{1}{2}} \end{pmatrix}$$

$$2x^2 + 2.5x + 1.75 \text{ solve, } x \rightarrow \begin{pmatrix} -0.625000000000000000 + .69597054535375274026 \times i \\ -0.625000000000000000 + .69597054535375274026 \times i \end{pmatrix} = \begin{pmatrix} -0.625 - 0.696i \\ -0.625 + 0.696i \end{pmatrix}$$

Figure 6.1 Roots obtained using the symbolic keyword ‘solve’

Mathcad numbers the angular grid lines in a polar plot from 0° to 360° .

Solve blocks were used in Mathcad file 221B1-03 for Chapter B1. The Newton–Raphson method was applied in Mathcad file 221C1-03 for Chapter C1.

This distinction, between exact and decimal expressions, may not seem very important, but it becomes more significant for a cubic polynomial. There is a formula giving the roots of a general cubic (we touched on this in Section 1), but it is much more complicated than the formula for the roots of a quadratic. Mathcad uses that formula if you use the symbolic keyword 'solve' to find the roots of a cubic.

Activity 6.5 Solving a quadratic and a cubic

Create a new (Normal) worksheet for this activity.

- (a) Use the symbolic keyword 'solve' to find the roots of the quadratic

$$2x^2 + \frac{5}{2}x + \frac{7}{4},$$

- (i) entering the coefficients as rationals;
- (ii) entering the coefficients as decimals.

With the vertical blue editing line at the right-hand end of the expression, click on the 'solve' button on the 'Symbolic' toolbar, then type x into its placeholder and either click elsewhere on the worksheet or press [Enter]. Alternatively, just type [Ctrl][Shift].solve, x .

- (b) Use the symbolic keyword 'solve' to find the roots of the cubic

$$x^3 - x + 2.$$

- (i) entering the coefficients as rationals;
- (ii) entering one coefficient as a decimal (for example, enter 2 as 2.0).

Comment

- (a) You should obtain the results shown in Figure 6.1.
- (b) In (i), you will obtain a large expression that spills off the right-hand side of the page and is not easy to read. In (ii), after clicking on the answer and entering =, you obtain the roots as -1.521 and $0.761 \pm 0.858i$ (to 3 decimal places).

If you click on the large exact expression given in (i) and enter =, Mathcad will give the value of that exact solution expressed as a decimal to 3 places, and so the same value as in (ii). You may need to scroll to the right to see this, though.

The situation for a quartic polynomial is similar to that for a cubic. There is a formula for the roots, and Mathcad employs this when the symbolic keyword 'solve' is used. The formula again produces very cumbersome answers in exact mode, but is usually an effective way of obtaining all four roots if the coefficients are entered as decimals.

For polynomials of order five or higher there is no general formula for the roots. In this case, Mathcad may respond in a variety of ways. It is quite good at recognising special situations where it is possible to give all the roots exactly, but in general this is not possible. Sometimes it gives answers with 20 decimal places, even though none of the coefficients is in decimal form.

Mathcad also has an alternative facility, called 'polyroots', which calculates all the roots of a polynomial, using an iterative procedure. Unlike the symbolic keyword 'solve', polyroots will not give exact answers, but then the exact expressions are often so large as to be unmanageable.

One advantage of polyroots is that it avoids the need to enter all the powers of x involved into the worksheet.

In most cases, polyroots is the most efficient way of finding all the roots of a polynomial. To use polyroots, we need first to enter the coefficients of the polynomial into Mathcad, as a vector. To do this, the coefficients can be entered either as a matrix with one column, or as subscripted variables. For example, to find all the roots of

$$x^5 + 3x^4 - 2x^3 - x^2 + 2x + 1,$$

we could use either of the approaches illustrated in Figure 6.2.

Notice that a_0 (at the top of the matrix) or b_0 gives the constant coefficient, which is 1 in this example; a_1 (second down in the matrix) or b_1 gives the coefficient of x (here 2), and so on. Entering =, after clicking on either of the expressions polyroots(a) or polyroots(b), gives the roots.

To define a matrix or subscripted variable, you can click on the appropriate button on the 'Matrix' toolbar, or type [Ctrl]M or [(left square bracket) respectively.

$$a = \begin{pmatrix} 1 \\ 2 \\ -1 \\ -2 \\ 3 \\ 1 \end{pmatrix}$$

$$b_0 = 1 \quad b_1 = 2 \quad b_2 = 1$$

$$b_3 = -2 \quad b_4 = 3 \quad b_5 = 1$$

polyroots(a)

polyroots(b)

Figure 6.2 Mathcad screens to find all the roots of $x^5 + 3x^4 - 2x^3 - x^2 + 2x + 1$

Activity 6.6 Finding the roots of a quintic

Create a new (Normal) worksheet for this activity (or continue with your worksheet for Activity 6.5).

- (a) Use polyroots to find all the roots of the quintic polynomial

$$x^5 + 3x^4 - 2x^3 - x^2 + 2x + 1.$$

- (b) What is the response from Mathcad if you enter the polynomial in part (a) and then apply the symbolic keyword 'solve',
- seeking exact solutions;
 - seeking approximate solutions, by putting a decimal point into one of the coefficients?

Comment

- (a) Figure 6.2 shows the two approaches that can be used here. We obtain the following five roots:

$$-3.454; \quad -0.541 \pm 0.161i; \quad 0.768 \pm 0.566i.$$

- (b) (i) If all the coefficients are entered as integers, then Mathcad's response is to give the roots correct to 20 decimal places.
- (ii) If one or more coefficients is entered as a decimal, then Mathcad gives the identical output to that described in (i).

Activity 6.7 Finding roots

In parts (a) and (b) below we give two results obtained by hand in Section 4 of the main text. Use Mathcad to confirm each of these results.

(a) In Activity 4.4, you found that 8 has the three cube roots

$$2; \quad -1 \pm i\sqrt{3}.$$

(b) In Activity 4.7, you found that $4i$ has the four fourth roots

$$1.307 + 0.541i; \quad -0.541 + 1.307i; \quad -1.307 - 0.541i; \quad 0.541 - 1.307i.$$

Comment

- (a) The cube roots of 8 are the roots of the polynomial $x^3 - 8$. The roots have been given exactly, and to obtain exact roots from Mathcad, we should use the symbolic keyword 'solve'. Since we have a cubic polynomial here, this should give all the roots, and it does. (Remember to enter the coefficients as integers.)
- (b) The fourth roots of $4i$ are the roots of $x^4 - 4i$. Use of polyroots gives the roots in the form above. (Enter the coefficients $a_4 = 1$, $a_3 = a_2 = a_1 = 0$ and $a_0 = -4i$.) The symbolic keyword 'solve' displays the solutions in an alternative format, which gives the same values to 3 decimal places after entering $\text{eng} =$. If either coefficient is entered as a decimal, then 'solve' finds only one of the four solutions.

Mathcad notes

Care is needed in Mathcad when redefining subscripted variables. Suppose that you define six variables, a_0, a_1, \dots, a_5 , but then later in the same worksheet, you redefine only five of them, a_0, a_1, \dots, a_4 . The sixth value a_5 is still defined, as it is 'inherited' from the first definition. (Note that while this problem may occur when defining separate subscripted variables, it does not occur if the definitions are made by defining a matrix a with one column.)

If you use the same worksheet here as for Activity 6.6, and enter the coefficients using separate subscripted variables, then you may inherit the coefficient $a_5 = 1$ from that work, and polyroots(a) may not give the answer you require! To avoid this problem, use a different name for the subscripted variables in this activity – see the Mathcad notes for an explanation.

You saw how to calculate the n th roots of unity in Section 4. There, we looked at some particular values of n . We can use the same approach to find a general formula for roots of unity. The n th roots of unity satisfy $z^n = 1$. If we express z in polar form, as $z = \langle r, \theta \rangle$ and 1 in polar form, as $\langle 1, 0 \rangle$, this equation gives

$$\langle 1, 0 \rangle = \langle r, \theta \rangle^n = \langle r^n, n\theta \rangle.$$

For this to hold, we need $r = 1$, and $n\theta$ to be a multiple of 2π . Thus, in polar form, the n th roots of unity are $\langle 1, 2k\pi/n \rangle$, where k takes the values $0, 1, \dots, n-1$. In Cartesian form, they are

$$\cos\left(\frac{2k\pi}{n}\right) + i \sin\left(\frac{2k\pi}{n}\right), \quad \text{for } k = 0, 1, \dots, n-1.$$

The next activity features a Mathcad file to find n th roots of unity.

Activity 6.8 Roots of unity

Open Mathcad file **221D1-02 Roots of unity**, and turn to page 2 of the worksheet. This page is set up to calculate the n th roots of unity (for a given value of n), both using the formula above and using polyroots, to enable you to compare the results. The coefficients a_0, a_1, \dots, a_{n-1} are defined by means of the Mathcad function $\text{if}(\text{condition}, p, q)$.

- Use this page to find the ninth roots of unity.
- Examine the Argand diagram plot of the n th roots of unity, on page 3 of the worksheet, for n equal to each of 5, 10, 25 and 50, and note any patterns that you observe. (You will need to set the value of n on page 2, in each case.)

Comment

- You need to set n equal to 9. The formula and polyroots give the same roots (though in different orders). The ninth roots of unity are

$$1, 0.766 \pm 0.643i, 0.174 \pm 0.985i, -0.5 \pm 0.866i, -0.940 \pm 0.342i.$$

- The roots of unity are always evenly spaced around the unit circle, as mentioned in Section 4. For larger values of n , the plot of corresponding points looks increasingly like a circle. (You may have noted other features.)

Mathcad notes

The tables of roots on page 2 of the worksheet have been formatted to display them in the same style. By default, entering $\text{polyroots}(a) =$ displays nine values or less within round brackets (in matrix form). To force Mathcad to display a table here, for any number of values, we have used the **Format** menu, **Result...**, and on the 'Display Options' tab, changed the 'Matrix display style' from 'Automatic' to 'Table'. Further changes have been made by clicking on the 'polyroots' table with the *right* mouse button, and choosing first 'Properties...', then 'Alignment' from the resulting mini-menu. In the table properties, column/row labels are not shown, and the alignment (of the expression $\text{polyroots}(a) =$ to the table values) is set to 'Top'. This alignment has also been set for the other two tables on the page, ' $k =$ ' and ' $z_k =$ '.

Now close file 221D1-02.

6.3 Complex exponentials and geometry

Complex exponentials are entered into Mathcad in just the same way as real exponentials, for example, by typing e^z (or $\exp(z)$).

Activity 6.9 Complex exponentials (Optional)

- In a new worksheet, set $z = 2 + 3i$, then evaluate e^z .
- With $z = 2 + 3i$, what are $|e^z|$ and $\arg(e^z)$? Use Mathcad to verify your answers.

This subsection will not be assessed

Comment

- (a) We obtain $e^{2+3i} = -7.315 + 1.043i$. (You found this result by hand in Activity 5.2.)
- (b) We have $e^z = e^{2+3i} = e^2(\cos(3) + i\sin(3))$. So
- $$|e^z| = e^2, \quad \arg(e^z) = 3.$$

Mathcad confirms these results. We obtain $|e^z| = 7.389$, and this equals e^2 to 3 decimal places. Symbolic evaluation (\rightarrow) of $|e^z|$ gives $\exp(2)$ directly.

We now use Mathcad to investigate sequences generated by the recurrence system

$$c_0 = 1, \quad c_{n+1} = kc_n \quad (n = 0, 1, 2, \dots), \quad (6.1)$$

where k is a fixed complex number. (We considered such sequences in Subsection 5.2 of the main text.)

Activity 6.10 Iterations with $|k|=1$ (Optional)

Open Mathcad file **221D1-03 Complex exponentials** and turn to page 2 of the worksheet. Here we consider the recurrence system (6.1) with k of the form $e^{i\theta}$, so that $|k| = 1$.

- (a) Consider first the sequence generated by the recurrence system (6.1) with $k = e^{i\pi/6}$.
- This sequence will eventually repeat itself. How do we know this?
 - How many iterations are needed before the sequence starts to repeat? Set N on page 2 of the worksheet to the smallest value that will plot all points of the sequence. Check that larger values of N plot nothing new.
- (b) For what values of θ in $k = e^{i\theta}$ does the sequence generated by the recurrence system (6.1) eventually repeat?
- (c) Decide on a value of θ for which the plot should look close to a circle. Choose a value of θ for which the sequence eventually repeats, and choose N large enough to show all the points of the sequence. Enter these values on page 2 of the worksheet, and check that they have the effect that you expected.
- (d) Decide on a value of θ for which the sequence does not eventually repeat. Examine the plot on page 2 for your chosen value of θ .

Comment

- (a) (i) You saw in Activity 5.5 of the main text that the sequence generated by the recurrence system (6.1) eventually repeats if and only if k is a root of unity. Now

$$(e^{i\pi/6})^{12} = e^{(i\pi/6) \times 12} = e^{2i\pi} = \cos(2\pi) + i\sin(2\pi) = 1,$$

so $e^{i\pi/6}$ is a twelfth root of unity.

- (ii) We have $c_{12} = k^{12} = 1 = c_0$, and after this the terms of the sequence repeat. So with $N = 11$ on page 2 of the worksheet, we see all points of the sequence plotted. With $N = 12$, the line joining c_{11} and c_{12} completes a regular 12-sided polygon, and the Mathcad plot looks the same for all higher values of N .

- (b) The sequence eventually repeats if k is a root of unity. Now $k = e^{i\theta}$ is a root of unity if $k^m = 1$ for some integer m ; that is, if we can find an integer m such that

$$(e^{i\theta})^m = 1, \quad \text{or} \quad e^{im\theta} = 1.$$

This is the case if $m\theta$ is equal to 2π , or to an integer multiple of 2π .

Thus the sequence generated by (6.1) with $k = e^{i\theta}$ eventually repeats if

$$\theta = 2p\pi/m,$$

where p and m ($\neq 0$) are integers.

- (c) The plot will eventually repeat if we choose $k = e^{i\theta}$ with $\theta = 2p\pi/m$. It will look close to a circle if we choose m reasonably large, say $m = 100$, and for simplicity we may as well take $p = 1$. So take k equal to, say, $e^{i\pi/50}$ and $N = 99$. (There are many other possible choices of k and N .)
- (d) Any value of k that is not a root of unity will produce a sequence that does not repeat. For example, for $k = e^{i\theta}$ with $\theta = 1$, and $N = 7$, we obtain the plot shown in Figure 6.3(a). You can see that k^7 is not equal to 1, and the plot does not return to its starting point. Nor does it return to 1 later. For example, the plot with $N = 13$ is shown in Figure 6.3(b). With larger values of N , as illustrated in Figure 6.3(c) with $N = 100$, it is much harder to make out what is happening, but the iteration never returns exactly to its starting point of $c_0 = 1$.

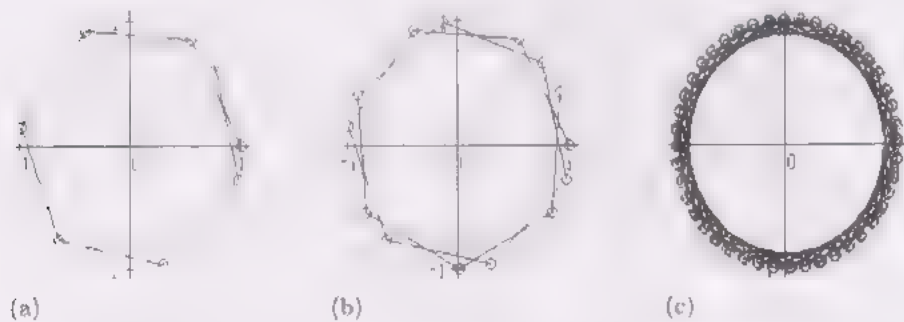


Figure 6.3 Plots of the sequence generated by recurrence system (6.1) with $k = e^i$, showing the sequence up to k^N with N equal to: (a) 7 (b) 13 (c) 100

Mathcad notes

To enter the complex exponential $re^{i\theta}$ in Mathcad, you can use the buttons on the 'Calculator' and 'Greek' toolbars, or type `r*e^1i*q[Ctrl]g`. (You must type 1i and include the multiplication * between the i and the θ .)

Activity 6.11 The twentieth roots of unity (Optional)

- (a) For what values of θ is $e^{i\theta}$ a twentieth root of unity?
- (b) Examine the sequences generated by the recurrence system (6.1) with $k = e^{ip\pi/10}$, where p is equal to each of

1, 2, 3, 4, 5, 6, 7, 17, 18, 19.

Note any points that you observe about the plots you obtain.

You should still be working with Mathcad file 221D1-03, on page 2 of the worksheet.

Comment

- (a) We have $(e^{i\theta})^{20} = 1$ if $e^{i20\theta} = 1$. This is the case if 20θ is an integer multiple of 2π ; that is, if $\theta = p\pi/10$, where p is an integer. (We obtain the complete set of twentieth roots of unity if p takes the values $0, 1, 2, \dots, 19$; other values of p just repeat one of these.)
- (b) Plots for $p = 1, 2$ and 3 are shown in Figure 6.4 (for $N = 20$ iterations). For $p = 1$ we see the twentieth roots of unity uniformly spaced around a unit circle, as we would expect. For $p = 2$, we obtain fewer points, 10 rather than 20. This is because $2(\pi/10) = \pi/5$, and $(e^{\pi/5})^{10} = e^{2\pi} = 1$. Hence $e^{2\pi/10}$ is a tenth root of unity (as well as being a twentieth root). So the plot in this case repeats itself after 10 iterations, and not all the twentieth roots of unity are visited. With $p = 3$, all the twentieth roots of unity are again visited by the plot. The order in which they are visited is different, though. With $p = 1$, the roots are visited in order as we go round the circle, that is, with m equal to $0, 1, 2, \dots, 19$ in $e^{im\pi/20}$. With $p = 3$, the roots are visited in the order

0, 3, 6, 9, 12, 15, 18, 1, 4, 7, 10, 13, 16, 19, 2, 5, 8, 11, 14, 17.

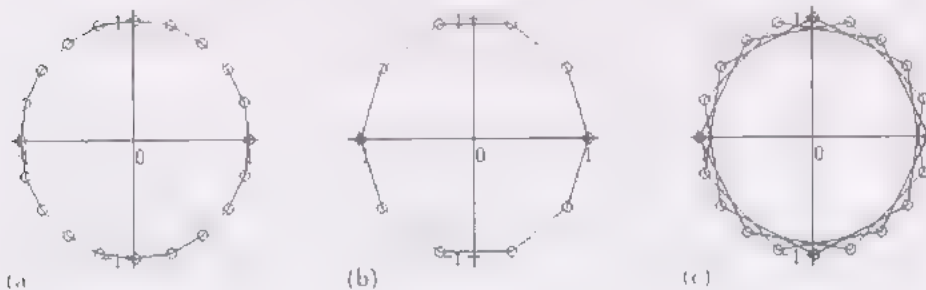


Figure 6.4 Plots of sequences generated by recurrence system (6.1) with $k = e^{ip\pi/10}$, for p equal to: (a) 1 (b) 2 (c) 3

With $p = 4$, we see only five roots. Here $4(\pi/10) = 2\pi/5$, and $e^{2i\pi/5}$ is a fifth root of unity.

With $p = 5$, we see only four roots, since $5(\pi/10) = \pi/2$ and $e^{i\pi/2}$ is a fourth root of unity.

With $p = 6$, we see 10 roots, since $6(\pi/10) = 3\pi/5$, and $e^{3i\pi/5}$ is a tenth root of unity. Here the roots are visited in the order (labelling round the circle): 0, 3, 6, 9, 2, 5, 8, 1, 4, 7.

With $p = 7$, all 20 roots are visited. Notice that $7\pi/10$ does not simplify at all, since 7 and 10 have no common factors. So here $e^{i7\pi/10}$ is a twentieth root of unity, but not an n th root for any smaller value of n .

With $p = 17$, we see the same plot as for $p = 3$. Although you cannot see it from the plot, in this case the roots are actually visited in the reverse of the order for $p = 3$, that is, 0, 17, 14, 11, \dots , 3.

With $p = 18$, we see the same plot as for $p = 2$; and for $p = 19$, we obtain the same plot as for $p = 1$.

If $|k|$ is not equal to 1, then the recurrence system (6.1) produces a spiral, as you saw in Subsection 5.2.

You should still be working with Mathcad file 221D1-03, on page 2 of the worksheet

Activity 6.12 Spirals (Optional)

Consider now sequences generated by the recurrence system (6.1) for a general complex number k , with polar form $\langle r, \theta \rangle$ where $r \neq 1$.

- (a) Examine the plot of the sequence with the following values of $k = \langle r, \theta \rangle$.

- (i) $\langle 1.1, \pi/6 \rangle$ (ii) $\langle \sqrt{2}, \pi/2 \rangle$ (iii) $\langle 1/\sqrt{2}, \pi/2 \rangle$
 (iv) $\langle \sqrt{2}, -\pi/2 \rangle$

In each case try two or three values for N . You will need to adjust the value of the graph scale variable s appropriately for each value of k .

- (b) Choose your own values of r and θ in $k = \langle r, \theta \rangle$. How does the spiral vary?

Comment

- (a) You saw plots of the spirals in these cases in Figures 5.2 and 5.3 of the main text.
 (b) With $r > 1$, the plot spirals outwards, and the larger r is, the more rapidly the spiral moves out. If $r < 1$, the spiral moves inwards. If $0 < \theta < \pi$ the spiral goes round anticlockwise, while if $-\pi < \theta < 0$ it goes round clockwise.

Finally, we look at plots of the complex-valued function $f(t) = r(t)e^{it}$. With $r(t) = a^t$, this plot gives a continuous spiral.

Activity 6.13 Continuous spirals (Optional)

Turn to page 3 of the worksheet, which shows a plot of the complex-valued function $f(t) = r(t)e^{it}$ ($t \geq 0$).

- (a) Examine the plot with $r(t) = a^t$, where a is equal to each of the following.

- (i) 1.1 (ii) 1.2 (iii) 0.9 (iv) 0.8 (v) 1

How does the plot vary? (You will need to adjust the value of the graph scale variable s in order to see the plots for (iii) and (iv) well.)

- (b) Examine the plot with $r(t)$ equal to each of the following.

- (i) t (ii) $1 + 0.2 \cos t$ (iii) $\ln t$ ($t \geq 1$)

How does the plot vary? (Again, adjust s appropriately.)

Comment

- (a) With $a > 1$, the plot is an increasing spiral. The rate of increase is faster if a is larger. With $a < 1$, the plot is a decreasing spiral. The rate of decrease is faster if a is smaller. With $a = 1$, the plot is a circle.
 (b) (i) With $r(t) = t$, we again see an increasing spiral.
 (ii) In this case the plot is a closed curve.
 (iii) Here you need to change the range for t , setting $T1 := 1$, because the domain given is $t \geq 1$. We see an increasing spiral, but the rate of increase becomes slower and slower. (This is particularly clear if you modify the range for t , to give a larger upper limit, such as $T2 := 40$.)

Now close file 221D1-03.

You should still be working with Mathcad file 221D1-03

Chapter D2, Section 5

Number theory and Mathcad

In this section, you will have an opportunity to develop your understanding of the concepts in the main text, to check some of your earlier calculations, and also to try out the methods with much larger numbers than your calculator can handle.

Mathcad can perform some arithmetic operations with very large integers by using symbolic evaluation, but we do not describe these capabilities until the end of the section.

5.1 The Division Algorithm

The Division Algorithm asserts that if a and n are integers, with n positive, then there are unique integers q and r such that

$$a = qn + r, \quad \text{with } 0 \leq r < n. \quad (5.1)$$

The number q is called the *quotient* and r is called the *remainder* of a , on division by n .

Equation (5.1) leads to formulas for q and r :

$$q = \text{floor}\left(\frac{a}{n}\right) \quad \text{and} \quad r = a - qn.$$

The first activity in this section asks you to try out these two formulas in Mathcad.

See Theorem 1.1 of the main text.

As you saw in Subsection 1.1 of the main text, $\text{floor}(x)$, also denoted by $[x]$, is the greatest integer less than or equal to x .

Activity 5.1 Quotients and remainders

- (a) By hand, find the quotient and remainder of
 (i) 32 on division by 6; (ii) -32 on division by 6.
 (b) Create a new (Normal) worksheet, and enter the following expressions.

$$\begin{aligned} a &= 32 & n &= 6 \\ q &:= \text{floor}\left(\frac{a}{n}\right) & r &:= a - qn \end{aligned}$$

Then enter $q=$ and $r=$ to evaluate these quantities. Change the value of a to -32 , and check that Mathcad gives the same answers that you obtained in part (a).

Make sure that you place the formula for r after that for q in the worksheet

Comment

- (a) (i) $q = 5, r = 2$ (ii) $q = -6, r = 4$
 (b) Mathcad gives the same values.

It is a good idea to enter some text to structure the worksheet you are creating in this and subsequent activities. For example, a title and some headings and comments might be useful.

Activity 5.1 shows that Mathcad can easily be used to find quotients and remainders. To investigate the behaviour of these quotients and remainders, it is convenient to introduce a pair of functions defined as follows.

$$\text{quot}(a, n) := \text{floor}\left(\frac{a}{n}\right) \qquad \text{rem}(a, n) := a - n \text{quot}(a, n)$$

Activity 5.2 Varying a and keeping n fixed

- Enter the functions above in your Mathcad worksheet, and check that $\text{quot}(-32, 6) = -6$ and $\text{rem}(-32, 6) = 4$.
- Describe how $\text{quot}(a, n)$ and $\text{rem}(a, n)$ behave when n is kept fixed and a is allowed to increase. It may help to consider an example, such as $n := 3$ and $a := -10, -9 \dots 10$, and to create tables or graphs for $\text{quot}(a, n)$ and $\text{rem}(a, n)$. (You may need to format graphs appropriately to show the behaviour clearly.)

Comment

- As a increases

- ◇ $\text{quot}(a, n)$ increases by 1 whenever a reaches a multiple of n , but is otherwise equal to its previous value;
- ◇ $\text{rem}(a, n)$ cycles repeatedly through the numbers $0, 1, 2, \dots, n-1$.

These statements are illustrated by the graphs in Figure 5.1.

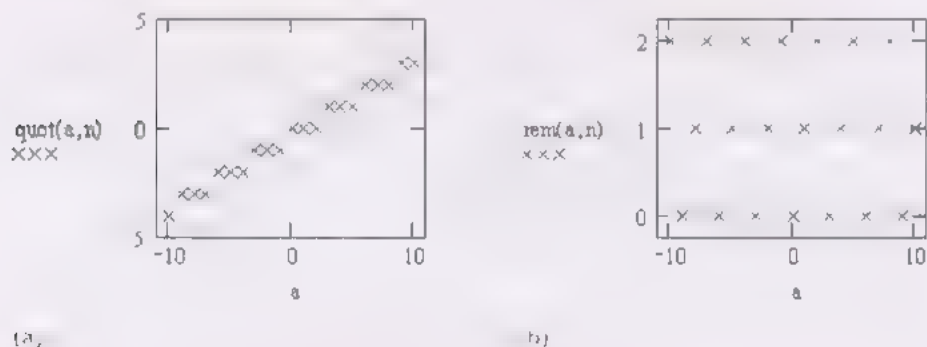


Figure 5.1 Graphs of the functions (a) quot , (b) rem

You may have wondered whether Mathcad has its own built-in functions for calculating quotients and remainders. In fact Mathcad has a function called `mod`, which can be used for finding remainders. This function has two arguments: it can be obtained by typing `mod(a, n)`.

Activity 5.3 The function `mod`

- Enter the following expressions in your worksheet, and then evaluate them by entering `=`.
 - `mod(32, 6)`
 - `mod(-32, 6)`
- Vary the numbers used as arguments in part (a). On the basis of the observed values, attempt to define the function `mod`.
- What happens when you try to evaluate `mod(ak, n)`, where $a = 3$, $k = 1000$ and $n = 13$?

Comment

(a) (i) $\text{mod}(32, 6) = 2$ (ii) $\text{mod}(-32, 6) = -2$

(b) Several illuminating examples are:

$$\text{mod}(0, 6) = 0, \quad \text{mod}(32, -6) = 2, \quad \text{mod}(-32, -6) = -2.$$

It seems from these examples that Mathcad evaluates $\text{mod}(a, n)$, where a and n are integers with $n \neq 0$, by first finding the remainder when $|a|$ is divided by $|n|$, and then giving this remainder the same sign as a .

Mathcad will also return a value for $\text{mod}(a, n)$ when a and n are not integers, but that does not concern us here.

(c) An error message is displayed: 'Found a number with a magnitude greater than 10^{307} while trying to evaluate this expression.'. Finding such remainders, when a^k is large, is addressed in Activities 5.4 and 5.6.

Save the worksheet that you have created, if you wish. Then close the file.

An alternative definition of the Mathcad function mod is as follows:

$\text{mod}(a, n)$ is the unique integer r satisfying

- ◇ $r < |n|$;
- ◇ $a = qn + r$, for some integer q ;
- ◇ r has the same sign as a .

This makes it clear that $\text{mod}(a, n)$ is a remainder of a on division by n , but for $a < 0$ it is *not* the remainder which is useful in number theory. However, we can use $\text{mod}(a, n)$ to find such remainders when a and n are both positive.

Warning: As you will see in Subsection 5.4, when evaluated symbolically (with \rightarrow) the Mathcad function mod *does* behave in the way required for number theory, always giving non-negative remainders!

5.2 Remainders of powers

In Section 1 of the main text two methods, here called algorithms, were described for finding the remainder of a^k on division by n , where a , k and n are positive integers. Both these algorithms – repeated multiplication and repeated squaring – are implemented in Mathcad file 221D2-01.

Repeated multiplication

To find the remainder of a^k on division by n , we calculate successively the remainders of $a^0, a^1, a^2, a^3, \dots$ on division by n , using a recurrence relation which expresses each remainder in terms of the previous one.

If we denote by r_i the remainder of a^i on division by n , then

$$r_i \equiv a^i \pmod{n},$$

so

$$r_i \equiv a \times a^{i-1} \equiv ar_{i-1} \pmod{n}.$$

Also, $r_0 \equiv a^0 \equiv 1 \pmod{n}$. Thus, there is a simple recurrence system for calculating the remainders $r_0, r_1, r_2, \dots, r_k$.

The sequence of remainders always shows a repeating pattern.

Activity 5.4 Repeated Multiplication Algorithm

Open Mathcad file **221D2-01 Remainders of powers**, and turn to page 2 of the worksheet. This implements the Repeated Multiplication Algorithm by means of a Mathcad program. The page is set up with $a = 3$, $k = 1000$ and $n = 13$, and shows that the remainder of $a^k = 3^{1000}$ on division by 13 is $r_k = 3$. The table of remainders illustrates the repeating pattern of values within the sequence $r_0, r_1, r_2, \dots, r_k$.

- (a) Use the worksheet to find the remainder on division of 5^{2000} by 21.
 (b) Experiment with various choices of a and n (keeping k fixed at 2000), to find repeating sequences of remainders with the following forms.
 (i) $1, r, r, r, \dots$ (ii) $1, r, s, r, s, \dots$ (iii) $1, r, s, t, r, s, t, \dots$

Comment

- (a) With $a = 5$, $k = 2000$ and $n = 21$, the required remainder is $r_{2000} = 4$. Note that the table shows the sequence

$$1, 5, 4, 20, 16, 17, 1, 5, 4, 20, 16, 17, \dots,$$

with a pattern which repeats after 6 terms. If you scroll across the table to $i = 2000$, you will see that the remainder $r_{2000} = 4$ appears there as well.

A 'by hand' check is as follows. Since $5^6 \equiv 1 \pmod{21}$, we obtain

$$5^{2000} \equiv 5^{6 \times 333 + 2} \equiv (5^6)^{333} \times 5^2 \equiv 5^2 \equiv 25 \equiv 4 \pmod{21}.$$

- (b) (i) $a = 4$, $n = 12$ gives remainders $1, 4, 4, \dots$
 (ii) $a = 3$, $n = 12$ gives remainders $1, 3, 9, 3, 9, \dots$
 (iii) $a = 2$, $n = 14$ gives remainders $1, 2, 4, 8, 2, 4, 8, \dots$

These answers are not unique.

The next activity revisits a result from Section 3 of the main text.

Activity 5.5 Experiment with primes

- (a) Use the worksheet again to experiment with various prime numbers for n , and positive integers a . (Keep $k = 1000$.) Notice from the table that 1 usually appears in the sequence of remainders, and try to explain this.
 (b) Try $n = 341$ (which is not prime) and $a = 2$, and check that in this case also, 1 appears in the sequence of remainders.

Comment

- (a) If n is a prime number p and a is not a multiple of p , then we expect 1 to appear in the sequence of remainders, by Fermat's Little Theorem (Theorem 3.2 in the main text):

Let p be a prime number, and let a be a positive integer which is not a multiple of p . Then $a^{p-1} \equiv 1 \pmod{p}$.

- (b) You should have found from the table that $2^{10} \equiv 1 \pmod{341}$, which can also be checked by hand. This shows that 1 may appear in the sequence of remainders, even when n is *not* a prime number.
-

You should still be working with Mathcad file 221D2-01, on page 2 of the worksheet.

$$2^{10} = 1024 = 3 \times 341 + 1$$

Repeated squaring

A more efficient algorithm for finding the remainder of a^k on division by n involves the steps set out below. (Some of the details are illustrated in the margin for the case $a^k = 14^{27}$, $n = 55$, discussed in Subsection 1.3 of the main text.)

- ◇ Represent k as a sum of powers of 2:

$$k = c_0 + c_1 \times 2^1 + c_2 \times 2^2 + \cdots + c_m \times 2^m, \quad (5.2)$$

where c_0, c_1, \dots, c_m are in \mathbb{Z}_2 and $c_m = 1$.

- ◇ Find the remainders $s_0, s_1, s_2, \dots, s_m$ on division by n of $a^1, a^2, a^4, \dots, a^{2^m}$, using repeated squaring:

$$s_i \equiv s_{i-1}^2 \pmod{n}.$$

- ◇ Find the remainder on division of a^k by n :

$$\begin{aligned} a^k &= a^{c_0} \times (a^2)^{c_1} \times (a^4)^{c_2} \times \cdots \times (a^{2^m})^{c_m} \\ &\equiv s_0^{c_0} \times s_1^{c_1} \times s_2^{c_2} \times \cdots \times s_m^{c_m} \pmod{n}, \end{aligned}$$

using repeated multiplication modulo n .

This algorithm is implemented on the next page of the Mathcad worksheet. It is a little complicated, particularly the first step which finds the representation of k as a sum of powers of 2, the so-called *binary representation* of k . We shall explain how the implementation of the algorithm works after you have used it in the next activity.

$$\begin{aligned} 27 &= 1 + 2 + 8 + 16 \\ &= 1 + 1 \times 2 + 0 \times 2^2 \\ &\quad + 1 \times 2^3 + 1 \times 2^4 \end{aligned}$$

For $a = 14$ we have, for example, $s_1 = 31$ and so

$$s_2 \equiv 31^2 \equiv 26 \pmod{55}.$$

$$\begin{aligned} 14^{27} &= 14^1 \times 14^2 \times 14^8 \times 14^{16} \\ &\equiv 14^1 \times 31^1 \times 16^1 \times 36^1 \\ &\pmod{55} \end{aligned}$$

Activity 5.6 Repeated Squaring Algorithm

Turn to page 3 of the worksheet. This implements the Repeated Squaring Algorithm by means of a Mathcad program. The page is set up with $a = 14$, $k = 27$ and $n = 55$, and shows that the remainder of $a^k = 14^{27}$ on division by 55 is $p = 9$. The table displays intermediate values generated by the algorithm.

Use the worksheet to find each of the following:

- the remainder of $2^{10\,000}$ on division by 10 001;
- the remainder of 2^{561} and of 3^{561} on division by 561.

Comment

- (a) Here you need to enter $a = 2$, $k = 10\,000$ and $n = 10\,001$. The algorithm gives the remainder as $p_m = 4674$, so $2^{10\,000} \equiv 4674 \pmod{10\,001}$.

(This result shows that 10 001 is *not* a prime number, because if it were then the remainder would have been 1, by Fermat's Little Theorem. As you saw in Subsection 3.3 of the main text, we have $10\,001 = 73 \times 137$.)

- (b) Here the remainders p_m are 2 and 3, respectively, so $2^{561} \equiv 2 \pmod{561}$ and $3^{561} \equiv 3 \pmod{561}$.

(This result suggests that $a^{561} \equiv a \pmod{561}$, for *every* positive integer a , even though 561 is not prime, and this is true. A proof of this fact can be based on the congruences

$$a^2 \equiv 1 \pmod{3}, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17},$$

which hold if a is coprime with 561.)

You should still be working with Mathcad file 221D2-01

The role of the sequence p_0, p_1, \dots, p_m , is described after this activity.

$$561 = 3 \times 11 \times 17$$

The rest of this subsection will not be assessed.

You are not expected to be able to construct such an algorithm, but if you have time then try to see how it works.

We now give an explanation of the program for the Repeated Squaring Algorithm, given on page 3 of the worksheet.

The input values a , k and n are declared for use in the program. The method of calculating the numbers c_0, c_1, \dots, c_m , in the binary representation (5.2) of k , differs from that used in Subsection 1.3 (it avoids having to find the largest power of 2 which is less than k). First note that $q_0 = k$ and $c_0 = \text{mod}(k, 2)$.

The numbers c_1, c_2, \dots, c_m are found by calculating the repeated quotients on division by 2:

$$q_1 = \text{floor}\left(\frac{1}{2}q_0\right) = c_1 + c_2 \times 2^1 + \dots + c_m 2^{m-1}, \quad \text{so } c_1 = \text{mod}(q_1, 2);$$

$$q_2 = \text{floor}\left(\frac{1}{2}q_1\right) = c_2 + \dots + c_m 2^{m-2}, \quad \text{so } c_2 = \text{mod}(q_2, 2);$$

$$q_m = \text{floor}\left(\frac{1}{2}q_{m-1}\right) = c_m, \quad \text{so } c_m = \text{mod}(q_m, 2).$$

The counter i keeps track of how many iterations of this type take place. The final iteration gives $q_i = 1$, and the variable m is defined as the corresponding value of i , so m denotes the number of iterations that have occurred.

These iterations take place within a 'while loop', which is the block of program steps with a solid vertical line to the left and headed by the line 'while $q_i > 1$ '. Also within this loop, Mathcad calculates by repeated squaring the remainders on division by n of a^2, a^4, \dots, a^{2^m} , which are denoted respectively by s_1, s_2, \dots, s_m . (The remainder of a on division by n is given, before the while loop starts, by $s_0 = \text{mod}(a, n)$.)

The values s_0, s_1, \dots, s_m are used to calculate the sequence of products

$$p_0 = s_0^{c_0}, \quad p_1 = s_0^{c_0} \times s_1^{c_1}, \dots, \quad p_m = s_0^{c_0} \times s_1^{c_1} \times \dots \times s_m^{c_m},$$

modulo n , again by iteration. The final product p_m is the required remainder.

The program also outputs the values of m and c_i, s_i, p_i ($i = 0, 1, \dots, m$), so details of the calculation can be displayed in a table.

Now close file 221D2-01.

5.3 Arithmetic in \mathbb{Z}_n

Mathcad's mod function makes it easy to obtain addition and multiplication tables for $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ since, for example,

$$a +_n b = \text{mod}(a + b, n), \quad \text{when } a, b \in \mathbb{Z}_n.$$

Activity 5.7 Addition and multiplication in \mathbb{Z}_n

Open Mathcad file **221D2-02 Modular arithmetic**, and turn to page 2 of the worksheet.

- Remind yourself of the overall pattern in addition tables for \mathbb{Z}_n . Try changing n to 9, 10 and 12, say.
- Change addition to multiplication in the definition of $p_{i,j}$, and use the table for multiplication in \mathbb{Z}_{11} to find the multiplicative inverse of 5 in \mathbb{Z}_{11} .
- Use the multiplication table for \mathbb{Z}_{26} to find the multiplicative inverses of 7 and 9 in \mathbb{Z}_{26} .
- Which rows of the multiplication table for \mathbb{Z}_{26} include 1 and therefore all of \mathbb{Z}_{26} ? What do you notice about each of these row numbers and the number 26? Relate your observations to Theorem 3.1 of the main text.

The multiplication will be displayed as $a \times b$, since this is the default (**Math** menu, **Options...**, 'Display') for viewing multiplications in this worksheet.

Comment

- The addition table for \mathbb{Z}_n has the 'constant diagonal' pattern.
- The multiplicative inverse of 5 in \mathbb{Z}_{11} is 9.
- The multiplicative inverse of 7 in \mathbb{Z}_{26} is 15, and the multiplicative inverse of 9 in \mathbb{Z}_{26} is 3.
- The rows of the multiplication table for \mathbb{Z}_{26} which include all of \mathbb{Z}_{26} are: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25. These are the only integers in \mathbb{Z}_{26} which are coprime with 26. These observations verify Theorem 3.1 of the main text for the case $n = 26$.

Finding multiplicative inverses in sets \mathbb{Z}_n is important, for example in Section 4 on cryptography. If n is not too large then multiplicative inverses can be read off from the appropriate multiplication table, but when n is larger a method based on Euclid's Algorithm is available.

Suppose that we wish to find the multiplicative inverse of a in \mathbb{Z}_n , where a and n are coprime. Euclid's Algorithm involves

- ◇ applying the Division Algorithm first to n and a , and then repeatedly to pairs of remainders until the remainder 0 occurs:

$$\left. \begin{array}{l} n = q_1 a + r_1 \\ a = q_2 r_1 + r_2 \\ r_1 = q_3 r_2 + r_3 \\ \vdots \\ r_{m-2} = q_m r_{m-1} + r_m \\ r_{m-1} = q_{m+1} r_m \end{array} \right\} \quad (5.3)$$

(since a and n are coprime, we must have $r_m = 1$);

- ◇ eliminating the remainders r_1, r_2, \dots, r_{m-1} from all but the last of the above equations, to obtain an equation of the form

$$ab = kn + 1, \quad \text{with } b \text{ in } \mathbb{Z}_n.$$

Then b is the required multiplicative inverse of a in \mathbb{Z}_n .

The algorithm for multiplicative inverses is the subject of the next activity.

Activity 5.8 Multiplicative Inverse Algorithm

You should still be working with Mathcad file 221D2-02.

Turn to page 3 of the worksheet. This implements the Multiplicative Inverse Algorithm by means of a Mathcad program. The page is set up with $a = 7$ and $n = 26$, and shows that the multiplicative inverse of 7 in \mathbb{Z}_{26} is $b = 15$. The tables display intermediate values generated by the algorithm.

Use the worksheet to find the multiplicative inverse of each of the following.

- (a) 8 in \mathbb{Z}_{19} (b) 19 in \mathbb{Z}_{100} (c) 75 in $\mathbb{Z}_{49\,139}$

Comment

(a) Setting a equal to 8 and n equal to 19 gives the multiplicative inverse of 8 in \mathbb{Z}_{19} to be 12.

(b) The multiplicative inverse of 19 in \mathbb{Z}_{100} is 79.

(c) The multiplicative inverse of 75 in $\mathbb{Z}_{49\,139}$ is 10 483.

An alternative method of finding the answer to part (a) is to use the fact that 19 is prime, so

$$8^{18} \equiv 1 \pmod{19},$$

by Fermat's Little Theorem. Hence the multiplicative inverse of 8 in \mathbb{Z}_{19} is congruent to 8^{17} modulo 19, and this can be calculated using, for example, the Repeated Squaring Algorithm. A similar approach can be used in part (c), because 49 139 is prime.

The rest of this subsection will not be assessed.

Again, you are not expected to be able to construct such algorithms.

We now explain the program for the Multiplicative Inverse Algorithm, given on page 3 of the worksheet. The quotients and remainders in Euclid's Algorithm are found by putting $r_0 = a$ and then using the iteration

$$\begin{aligned} r_1 &= \text{mod}(n, a), & q_1 &= \text{floor}\left(\frac{n}{a}\right), \\ r_i &= \text{mod}(r_{i-2}, r_{i-1}), & q_i &= \text{floor}\left(\frac{r_{i-2}}{r_{i-1}}\right). \end{aligned}$$

The iteration continues while $r_i > 1$, after which m is put equal to the final value of i .

We know that $r_m = 1$ (provided that a and n are coprime, as assumed). The other remainders r_i are eliminated from equations (5.3) by multiplying by suitable constants c_1, c_2, \dots, c_{m+1} , and then adding up all $m + 1$ equations. To eliminate the r_j (for $j < m$) we require the constants to satisfy

$$c_{j+2} = q_{j+1}c_{j+1} + c_j.$$

Thus we want

$$c_j = -q_{j+1}c_{j+1} + c_{j+2}, \quad \text{for } j = 1, 2, \dots, m-1. \quad (5.4)$$

The remaining equation, of terms obtained by summing $m + 1$ equations as above but not eliminated by equations (5.4), is

$$c_1n + c_2a = c_1q_1a + (c_m + c_{m+1}q_{m+1})r_m.$$

We know that $r_m = 1$, so if we choose $c_m = 1$ and $c_{m+1} = 0$, then this becomes

$$\begin{aligned} c_1n + c_2a &= c_1q_1a + 1; & \text{that is,} \\ a(-c_1q_1 + c_2) &= (-c_1)n + 1. \end{aligned}$$

Defining $c_0 = -q_1 c_1 + c_2$ gives $ac_0 \equiv 1 \pmod{n}$, but it also gives an equation that fits the pattern of equations (5.4) for $j = 0$. Thus we have the recurrence system

$$c_{m+1} = 0, \quad c_m = 1, \\ c_j = -q_{j+1}c_{j+1} + c_{j+2}, \quad \text{for } j = m-1, m-2, \dots, 0.$$

This recurrence system is implemented in the Mathcad program.

Since $ac_0 \equiv 1 \pmod{n}$, the multiplicative inverse b of a in \mathbb{Z}_n is congruent to c_0 modulo n ; that is,

$$b = c_0 - n \text{ floor} \left(\frac{c_0}{n} \right)$$

The value of b is output by the program. The values of m , r_i , q_i and c_j are also output, so the details of the calculation can be displayed in two tables.

Now close file 221D2-02.

5.4 Multiple precision arithmetic

In Section 4 of the main text, you saw how arithmetic with large integers is used in cryptography. In particular, you saw the relevance of large prime numbers to a method of public key cryptography based on Fermat's Little Theorem. Symbolic evaluation in Mathcad can be used to perform arithmetic with large integers, so-called *multiple precision arithmetic*, and also to discover large prime numbers.

Arithmetic

For most numerical calculations, Mathcad maintains 15 digits of precision. However, for symbolic evaluations, basic arithmetic operations can be performed with rational numbers to many hundreds of digits of precision.

Activity 5.9 Arithmetic and mod with the symbolic processor

Create a new (Numeric) worksheet. Enter each of the following expressions, then evaluate it symbolically, either by clicking on the \rightarrow button on the Symbolic toolbar or by typing [Ctrl]... the keyboard alternative.

- (a) $111\,111\,111\,111 + 333\,333\,333\,333$
 (b) $111\,111\,111\,111 - 333\,333\,333\,333$
 (c) $111\,111\,111\,111 \times 333\,333\,333\,333$
 (d) $\frac{111\,111\,111\,111}{333\,333\,333\,333}$
 (e) 2^{60} (f) $25!$ (g) $\frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6}$ (h) $\text{mod}(-7, 4)$
 (i) $\text{mod}(2^{10\,000}, 10\,001)$

Care is needed in Mathcad when entering large numbers and reading them in answers. The digits are displayed in a long string – Mathcad does *not* help by grouping them in threes, with gaps between, as is usual in text.

To enter the factorial in part (f), click on the $n!$ button on the 'Calculator' toolbar, or type $!$ (given by [Shift]1).

Comment

The answers provided by Mathcad are as follows.

- (a) 444 444 444 444 (b) -222 222 222 222
 (c) 37 037 037 036 962 962 962 963 (d) $\frac{1}{3}$ (e) 1 125 899 906 842 624
 (f) 15 511 210 043 330 985 984 000 000 (g) $\frac{29}{20}$
 (h) 1 (Check that evaluating $\text{mod}(-7, 4)$ numerically gives the value -3.)
 (i) 4674

Factorisation

A positive integer can be expressed as a product of powers of prime numbers, by using the symbolic keyword 'factor'.

Activity 5.10 Factorisation

In this activity, use the worksheet that you created for Activity 5.9

Enter each of the following integers, and apply the symbolic keyword 'factor' to it. To do this, either click on the 'factor' button on the 'Symbolic' toolbar, followed by pressing [Backspace] twice to remove the unwanted placeholder, or type [Ctrl] [Shift] .factor .

- (a) 10 001 (b) 3 220 422 643 (c) 50!

Comment

- (a) $10\,001 = 73 \times 137$ (b) $3\,220\,422\,643 = 65\,537 \times 49\,139$
 (c) $50! = 2^{47} \times 3^{22} \times 5^{12} \times 7^8 \times 11^4 \times 13^3 \times 17^2 \times 19^2 \times 23^2 \times 29 \times 31$
 $\quad \times 37 \times 41 \times 43 \times 47$

There is much interest in discovering large prime numbers. By applying symbolic evaluation in Mathcad to suitable large integers, large primes may be found. A useful rule of thumb here is that

if an integer n has only small prime factors, then some nearby integer may well have large ones.

So it is a good idea to try factorising numbers of the forms $2^n \pm 1$, $3^n \pm 1$, etc. For example, applying the symbolic keyword 'factor' to $2^{45} + 1$ gives

$$2^{45} + 1 = 3^3 \times 11 \times 19 \times 331 \times 18\,837\,001;$$

hence 18 837 001 is prime.

The largest known prime number (in 2003) is $2^{13\,466\,917} - 1$, which has more than four million digits. It is one of the family of Mersenne prime numbers. These are all of the form $2^p - 1$, where p is a prime number, and they are found by applying a special test to numbers of this form.

In general, it is much harder to factorise large numbers than it is to perform basic arithmetic operations with them. Some large numbers, like those of the form 10^n , factorise very quickly, but most do not. As you saw in Section 4 of the main text, this fact makes it possible to base ciphers on large numbers which are the product of two large prime numbers.

Save the worksheet that you have created, if you wish. Then close the file.

If you are tempted to try calculations like these, then remember to save your work at each stage, because Mathcad may be unable to cope with huge calculations. (Mathcad's symbolic evaluations can handle numbers with about 10 000 digits.)

Chapter D3, Section 1

Symmetry

1.3 Using symmetries

In Section 1 of the main text, you saw how the pattern, or structure, of a plane set X can be described by finding its set of symmetries $S(X)$. In the optional Mathcad files for this chapter you will see how knowing the symmetries can be helpful if you wish to plot the plane set using a computer package. These files are self-contained and may be worked through after reading the following introductory remarks.

This subsection will not be assessed.

First, in file 221D3-01, we explain how Mathcad can be used to plot a path made up of line segments placed end-to-end. Such a path is called a *piecewise linear path*, or PLP for short, and it is defined by prescribing a finite sequence of points in the plane, say $p(i)$, $i = 0, 1, \dots, n$ and then joining $p(0)$ to $p(1)$, $p(1)$ to $p(2)$ and so on, using line segments.

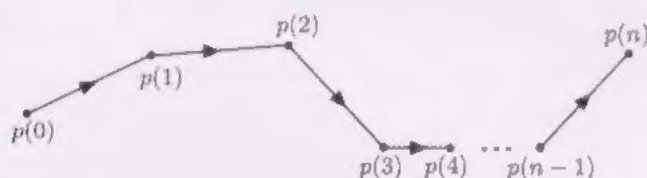
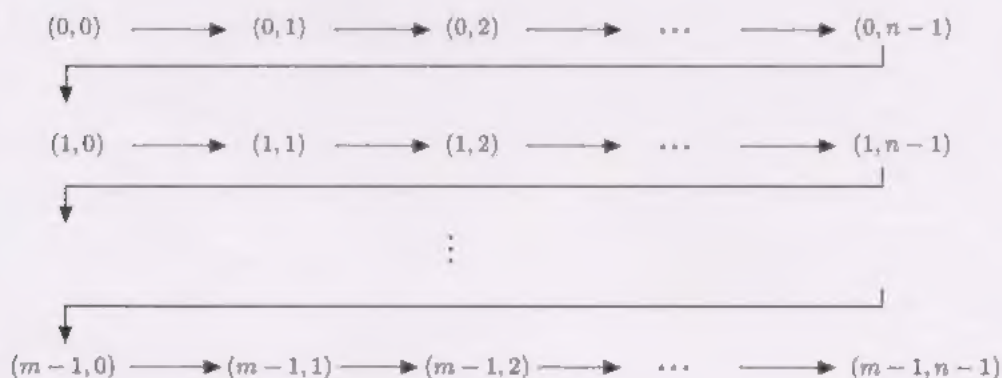


Figure 1.20 A piecewise linear path

In this diagram, the arrows show the direction in which the line segments are plotted. Notice that a PLP with n line segments requires $n + 1$ points, or *vertices*, to determine it.

One way to prescribe the vertices of a PLP in Mathcad is to take i to be the range variable $i := 0, 1 \dots n$, and define $p(i)$ to be a function of i whose values are vectors, that is points in the plane. The corresponding PLP can then be plotted using an X - Y Plot, with the components $p(i)_0$ and $p(i)_1$ as the arguments on the x -axis and y -axis, respectively, and with the trace type set to 'lines'.

In file 221D3-02 we use Mathcad to plot a symmetric PLP corresponding to a vector-valued function $SP(j, i)$ of two range variables $j := 0, 1 \dots m - 1$ and $i := 0, 1 \dots n - 1$, by going through the range variables in the following order.



This facility makes it possible to plot plane sets with many symmetries, such as the snowflake and rose window shown below. We do this in files 221D3-02 and 221D3-03.

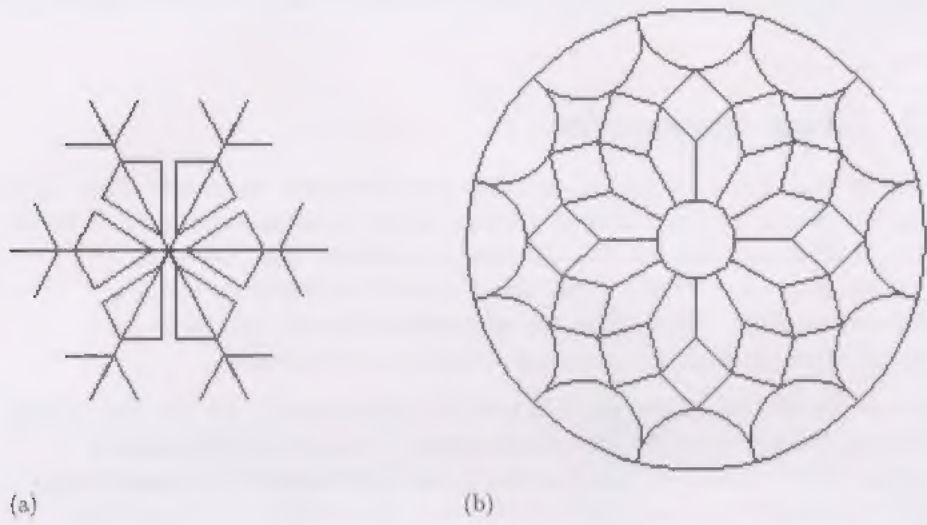


Figure 1.21 (a) A snowflake (b) A rose window



The Open University
ISBN 0 7492 6650 3